

WE CLAIM:

1. A method of processing a routing information in a packet data network, said method comprising the steps of:

extracting said routing information from a received message at a border between a first network and a second network;

adding at least one invalid entry to first-network entries of said routing information, said first-network entries relating to a routing path of said message within said first network;

generating an encrypted routing information by encrypting said at least one invalid entry and said first-network entries by using an own token at least for each of said first-network entries;

replacing said routing information of said received message by said encrypted routing information; and

forwarding said received message with said encrypted routing information to said second network.

2. The method according to claim 1, further comprising the step of:

providing said routing information in a routing header of said message.

3. The method according to claim 2, further comprising the step of:

providing said routing header comprising a Record-Route header of a Session Initiation Protocol message and a Service-Route header as specified for the Session Initiation Protocol.

4. The method according to claim 1, further comprising the step of:

processing said routing information using a topology hiding method.

5. The method according to claim 4, wherein, in said processing step, said topology hiding method is applied in response to a user identity marked with a predetermined information.

6. The method according to claim 4, wherein, in said processing step, said topology hiding method is applied in response to a network identity.

7. The method according to claim 1, further comprising the step of: marking said at least one added invalid entry.

8. The method according to claim 1, further comprising the step of: providing each of said first-network entries comprising at least one of name and address information of a network node through which said received message has been routed.

9. The method according to claim 1, further comprising the step of: providing said border between said first and second networks, wherein said border is defined at a gateway device which said message traverses on a connection between said first and second networks.

10. A network device for processing routing information in a packet data network, said device comprising:

extracting means for extracting said routing information from a received message at a border between a first network and a second network;

adding means for adding at least one invalid entry to first-network entries of said routing information, said first-network entries relating to a routing path of said message within said first network;

encrypting means for generating an encrypted routing information by encrypting said at least one invalid entry and said first-network entries by using an own token at least for each of said first-network entries;

replacing means for replacing said routing information of said received message by said encrypted routing information; and

forwarding means for forwarding said received message with said encrypted routing information to said second network.

11. The network device according to claim 10, wherein said network device further comprises one of an Interrogating Call Session Control Function and a Topology Hiding Gateway function.

12. The network device according to claim 10, wherein said packet data network further comprises an IP Multimedia Subsystem.

13. The network device according to claim 10, wherein said border between said first and second networks is defined at said network device.

14. A method of processing a routing information in a packet data network, said method comprising the steps of:

extracting said routing information from a received message at a border between a first network and a second network;

generating a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network entry;

replacing said routing information of said received message by said decrypted and reversed routing information; and

forwarding said received message with said decrypted and reversed routing information to said second network.

15. The method according to claim 14, further comprising the step of:

conveying said routing information in a routing header of said message.

16. The method according to claim 15, wherein said routing header comprises at least one of a Route header and a Via header of a Session Initiation Protocol message.

17. The method according to any claim 14, further comprising:
using a topology hiding method.

18. The method according to claim 17, further comprising the step of:

applying said topology hiding method in response to a user identity marked with a predetermined information.

19. The method according to claim 17, further comprising the step of:

applying said topology hiding method in response to a network identity.

20. The method according to claim 14, wherein:

said tokenized second-network entry comprises at least one of an encrypted name and encrypted address information of a sequence of network nodes through which said received message has been routed.

21. The method according to claim 14, further comprising the steps of:

marking a tokenized network entry of at least one of an incoming and an outgoing tokenizing network node; and

suppressing said reversing step at outgoing tokenizing network nodes.

22. The method according to claim 14, further comprising the steps of:

marking a tokenized network entry of at least one of an incoming and an outgoing tokenizing network node; and

reversing network entries at incoming tokenizing network nodes before encryption.

23. The method according to claim 14, wherein:

said border between said first and second networks is defined at a gateway device which said message traverses on a connection between said first and second networks.

24. A network device for processing routing information in a packet data network, said device comprising:

extracting means for extracting said routing information from a received message at a border between a first network and a second network;

decrypting and reversing means for generating a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network entry;

replacing means for replacing said routing information of said received message by said decrypted and reversed routing information; and

forwarding means for forwarding said received message with said decrypted and reversed routing information to said second network.

25. The network device according to claim 24, further comprising one of an Interrogating Call Session Control Function and a Topology Hiding Gateway function.

26. The network device according to claim 24, wherein said packet data network comprises an IP Multimedia Subsystem.

27. The network device according to claim 24, wherein said network device is configured to suppress reversing of said decrypting and reversing means when said routing information indicates that said network device is an outgoing tokenizing network node.

28. The network device according to claim 24, wherein said network device is configured to reverse network entries before encryption when said routing information indicates that said network device is an incoming tokenizing network node.

29. The network device according to claim 24, wherein said border between said first and second networks is defined at said network device.

30. A network device for processing routing information in a packet data network, said device comprising:

- an extraction unit configured to extract said routing information from a received message at a border between a first network and a second network;

- an adding unit, operably connected to said extraction unit, and configured to add at least one invalid entry to first-network entries of said routing information, said first-network entries relating to a routing path of said message within said first network;

- an encrypting unit, operably connected to said extraction unit, and configured to generate encrypted routing information by encrypting said at least one invalid entry and said first-network entries by using an own token at least for each of said first-network entries;

a replacing unit, operably connected to said extraction unit, and configured to replace said routing information of said received message by said encrypted routing information; and

a forwarding unit, operably connected to said extraction unit, and configured to forward said received message with said encrypted routing information to said second network.

31. A network device for processing routing information in a packet data network, said device comprising:

an extracting unit configured to extract said routing information from a received message at a border between a first network and a second network;

a decrypting and reversing unit, operably connected to said extracting unit, and configured to generate a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network entry;

a replacing unit, operably connected to said extracting unit, and configured to replace said routing information of said received message by said decrypted and reversed routing information; and

a forwarding unit, operably connected to said extracting unit, and configured to forward said received message with said decrypted and reversed routing information to said second network.